UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Records Seized from KYL International, LLC
d/b/a Nagoya Japanese Restaurant
1155 W. Arbrook Boulevard, Arlington, Texas 76015

Case No. 4:16-MJ-717

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
26 U.S.C. § 7206 (1)	Fraud and False Statement

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Robert De Los Santos, IRS-CI
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/4/16

Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton
Printed name and title

AFFIDAVIT OF ROBERT DE LOS SANTOS

INTRODUCTION

1. I, Roberto Jose De Los Santos, Special Agent of the United States Department of Treasury, Internal Revenue Service, Criminal Investigation (IRS-CI), being duly sworn, state:

2. This affidavit is submitted in support of an application for a search warrant for items seized, further described in Attachment A, through a search warrant executed by The Texas State Comptroller–Criminal Investigation Division (Comptroller-CID) on January 27, 2015, which are presently located at the offices of the IRS-Criminal Investigation located at 819 Taylor Street, Room 6A18, Fort Worth, Texas 76102, in the Northern District of Texas, for evidence of violations of 26 U.S.C. §§ 7201, 7206(2) and 7212(2), and 18 U.S.C. § 371 ("the Subject Offenses"), all of which has occurred or is occurring, or involves overt acts occurring in the Northern Judicial District of Texas.

AFFIANT EXPERIENCE

3. I have been a Special Agent with IRS-CI since 2010. I am presently assigned to the Fort Worth, Texas office.

4. As part of my duties as an Internal Revenue Service Special Agent, I investigate criminal violations relating to financial and tax fraud. I have had substantial training and experience in investigating financial fraud, including tax violations. I have participated in multiple financial investigations involving violations of Titles 18, 26 and 31 of the United States Code, and I also have

participated in the execution of multiple federal search warrants for financial and other business records as part of these investigations.

5. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of the Subject Offenses are located on the computer/storage media and documents secured from KYL International, LLC (KYL), d/b/a Nagoya Japanese Restaurant, during a search warrant executed by Comptroller-CID.

6. IRS-CI is conducting this investigation. The evidence of criminal activity conducted by KYL and one of the managing partners, Kevin Chau, has been gathered as a result of a search warrant executed by Comptroller-CID. The information contained within this affidavit is based upon by personal knowledge, information received from other IRS Special Agents and Comptroller-CID investigators and auditors, pubic record checks, a review of Federal income tax returns, and information gained from my training and experience.

BACKGROUND OF INVESTIGATION

7. A point of sales (POS) system is computer equipment used by retail sales outlets, including restaurants, which includes software that can track sales and

inventories, and can produce sales and other accounting reports. POS equipment can be linked to create a network or operate as a standalone electronic register.

8. In general, in a restaurant setting, when an order is placed, it is inputted through a POS touch-screen terminal, which forwards the order to the kitchen and creates a record of the order in the electronic computer files of the POS system. When the transaction is completed and the customer pays for the meal, the POS system records how the meal was paid for and the order is closed out on the POS system. The POS system generally captures and stores information regarding sales, including sales by item and sales by certain time periods including by day, week and month and annual sales. To protect users against system crashes and loss of data, the databases and computer files which capture information about restaurant sales can be stored and backed up on POS system equipment at the restaurant site, on computers located at the vendor's place of business, on internet based servers, on external computer storage, or on any other electronic storage devices.

9. The data captured by POS systems can generate sales reports or be exported to computer spreadsheets that can be used to compute taxes owed to the IRS and other taxing authorities.

10. The retail sales transaction data can be altered through the use of an "automatic sales suppression device." This is a device or software program that falsifies an electronic record, including transaction data or a transaction report, of an electronic cash register or other POS system. The term includes a device that

carries the software program or an Internet link to the software program. It can also be altered through the use of "phantom-ware," which is a hidden programming option that is embedded in the operating system of an electronic cash register and that may be used to create a second set of transaction reports or to eliminate or manipulate an original transaction report, which may or may not be preserved in a digital format, to represent the original or manipulated report of a transaction in the electronic cash register.

11. Since September 1, 2013, it has been a criminal offense in Texas if a person knowingly sells, purchases, transfers, uses, or possesses an automated sales suppression device or phantom-ware. It is a state jail felony defined in Texas Business and Commerce Code Section 326.002.

FACTS SUPPORTING PROBABLE CAUSE

12. I was informed by Comptroller-CID investigator John T. Bermea that on July 7, 2014, Comptroller Auditor Justin Driscoll was contacted by Warren Klomp, a District Administrator with the California Board of Equalization, that KYL was a customer of the POS system OPUS software. Warren Klomp supervises auditors in California and on at least 13 occasions has found OPUS software during tax audits that included a feature that allows the deletion of sales and reorganization of the data to conceal sales to evade tax consequences. Warren Klomp has developed a training program on how to identify phantom-ware products such as OPUS and is recognized internationally as an expert on phantom-ware. The training hosted by Warren Klomp is attended by tax officials from

several states and Canada. Warren Klomp had previously provided information and training materials to Auditor Justin Driscoll that shows that OPUS software has been found to include the aforementioned hidden feature that allows removal of sales records, which meets the definition of phantom-ware in Chapter 326 of the Texas Business and Commerce Code.

13. I was informed by Comptroller-CID investigator John T. Bermea that on July 17, 2014, he met with Comptroller Auditor Justin Driscoll. Auditor Justin Driscoll advised John T. Bermea that he had conducted a mixed-beverage gross receipts audit of KYL located at 1155 W. Arbrook Boulevard, Arlington, Texas. Auditor Justin Driscoll explained that during his audit he was given access to the POS system by Kevin Chau, managing partner of KYL. With permission from Kevin Chau, Auditor Justin Driscoll copied the database files from the POS computer, which used OPUS software, to a removable storage device. The database contained an original, unsuppressed, database as well as an altered, suppressed, database for July 2008 through March 2014. Auditor Justin Driscoll was also provided copies of KYL's partnership tax returns for the years 2011, 2012 and 2013.

14. Auditor Justin Driscoll also found historical sales data ranging from September 2000 through March 2002 which dates back to the former location of Nagoya Japanese Restaurant. Texas Secretary of State records, and Texas State Comptroller franchise tax filing records list that Kevin Chau was formerly President of Cheung Kong International, Inc. which did business as Nagoya

Japanese Restaurant at 4040 S. Cooper Street, Arlington, Texas from June 2000 to January 2008. The historical data shows that after September 2001 there was a significant decrease in the number of customers that paid cash in relation to previous months. Auditor Justin Driscoll found from the historical data that Nagoya Japanese Restaurant had cash sales of $20,922.80 (gross sales $93,237) in February 2001 but only $4,327.75 of cash sales (gross sales $81,607) in February 2002. This shows a 79% drop in cash sales however gross sales only dropped 9%. In the same comparison, there were 407 less cash sale tickets, while the number of total credit card sales went up by only three. This could indicate management was using phantom-ware to delete sales data as early as September 2001.

15. Further analysis of the current KYL POS databases revealed that for the period of July 2008 through March 2014, on a daily basis, approximately 50% to 95% of the cash sales were being removed from the sales totals, which averages approximately $750 a day. Auditor Justin Driscoll found the percentages through comparison of amounts reported to the Comptroller's office through tax fillings and the point of sale database information that Nagoya was using OPUS phantom-ware to suppress sales data and that sales tax was collected and not remitted totaling $117,631 (17% of total tax collected) and that approximately $15,000 mixed beverage tax went unreported. This under reporting of the tax owed is a result of approximately $1,610,573 in cash sales being suppressed for the period of July 2008 through March 2014. Auditor Justin Driscoll discovered that in addition to removing records of the cash sales, OPUS phantom-ware enables restaurant

management to reorder the ticket numbers, which then conceals the missing cash sale tickets.

16. On January 27, 2015, Comptroller-CID executed a search warrant on KYL, located in Arlington, Texas. During the search warrant, Auditor Justin Driscoll and CID investigator Ty Bermea interviewed Kevin Chau. Kevin Chau stated that he operates and runs Nagoya restaurant daily. The other partners are silent partners except for one who is a sushi chef.

17. Federal Partnership Tax returns, Form 1165, show the following partners and their ownership percentages: Kevin Chau (50% owner), Jonathan Lam (30% owner), Ann Laichun Lam (15% owner), and Yuet Yu (5% owner).

18. Kevin Chau installed Opus software as Nagoya's POS system. He purchased the software from California. Kevin Chau deals mostly with a person named "Jimmy" at Opus. "Jimmy" trained Kevin Chau on how to operate OPUS. "Jimmy" has remote access to Kevin Chau's software.

19. Kevin Chau admitted to suppressing cash sales from the POS system. On a daily average Kevin Chau would suppress a couple hundred dollars, but this was not done daily. Kevin Chau is the only person with manager access to Opus. The other employees have regular access. Kevin Chau stated that none of the other partners are aware of Kevin Chau suppressing cash sales. No one taught Kevin Chau how to suppress cash, he learned on his own. Kevin Chau claims that he did not know that suppressing cash was illegal.

20. Kevin Chau claims that all of Nagoya's income is reported on the partnership returns. He then stated that some cash was not reported. He provided all his daily printouts to his CPA Jim Xu. Kevin Chau is not aware if the suppressed cash is included in the daily printout reports he provided the CPA. The CPA does not have access to the restaurant's computer.

21. Kevin Chau used the suppressed cash to pay employees tips, fund the petty cash, and cash for himself. Kevin Chau did not use the suppressed cash to pay any of the other partners.

22. The computer/media items located during the search warrant of KYL were analyzed by CID investigator John T Bermea. His review of the computer hard drive showed that the original database was not the same as the database provided to Auditor Justin Driscoll. The database was altered and only showed sales transactions that reflected the sales reported on the partnership tax returns. Discs and flash drives containing yearly backups, January 2009 through January 2013, of the suppressed and unsuppressed databases were discovered and are the same databases that were acquired by Auditor Justin Driscoll during his audit of KYL.

23. Below is a Summary of what was reported to IRS on Forms 1065 for KYL International. The gross sales shown on the tax returns correspond to the suppressed database, which does not include the deleted cash transactions.

Tax Year	Gross Sales	Total Income	Salaries and Wages	Total Deductions	Business Income
2010	$1,269,400	$598,926	$148,656	$552,287	$46,639
2011	$1,354,407	$626,391	$157,423	$554,422	$71,969
2012	$1,377,596	$709,488	$167,969	$581,693	$127,795
2013	$1,454,479	$739,787	$170,120	$606,003	$133,784

Using the records provided by Auditor Justin Driscoll the following true gross sales and suppressed cash sales per year are summarized below:

Year	**Gross Receipts** (Original Database)	**Reported Gross Receipts** (Reported Income)	**Unreported Cash** (Gross Receipts minus Reported Gross Receipts)
2010	$1,539,207.17	$1,269,400	$269,807.17
2011	$1,650,700.77	$1,354,407	$296,293.77
2012	$1,642,661.65	$1,377,596	$265,065.65
2013	$1,721,408.33	$1,454,479	$266,929.33
Totals	**$6,553,977.92**	**$5,455,882**	**$1,098,095.92**

24. A review of Kevin Chau's personal returns does not show additional income in the amount of the unreported cash.

CONCLUSION

25. Based upon Affiants experience and knowledge in investigating violations of Title 18 and 26 of the United States Code and Internal Revenue laws, in preparing Affidavits for the execution of search warrants, participating in the execution of numerous search warrants at both residences and businesses and from conversations with other agents who are also involved in the investigation of like

violations, Affiant knows that, in addition to the OPUS "phantom-ware" software that allows the deletion of sales and reorganization of the data to conceal sales for tax evasion, records of the types sought including sales reports, invoices, receipts, employee work schedules, Federal and State tax documents, bank and credit card statements, and other financial and business records are often maintained on paper and in electronic form and stored on a variety of computer, and digital electronic storage devices to include flash drives, hard disk drives, floppy disks, and optical storage media. It is also known, based upon Affiant's experience in dealing with these various forms of electronic evidence and in Affiant's conversations with other agents directly involved in the processing and recovery of electronic evidence, that these storage devices can store data for a large period of time and that such data, even when erased, may be retrievable. Based upon this, it is reasonable to believe that records constituting evidence of crimes outlined herein will be maintained and found in the items seized by the Texas State Comptroller-CID as fully described in Attachment A. The items were seized by The Texas Comptroller-CID on January 27, 2015 and remained in the care, custody and control of The Texas Comptroller-CID until they were transferred into the custody of the IRS-Criminal Investigation at 819 Taylor Street, Room 6A18, Fort Worth, TX 76102.

26. Therefore, I respectfully request that a warrant be issued authorizing the imaging and search of the items described in Attachment A for any fruits, instrumentalities, or evidence of the violations specified above, and the seizure of all fruits, instrumentalities, and evidence, as further described in Attachment B.

Special Agent - Robert J. De Los Santos
Internal Revenue Service
Criminal Investigation

Sworn and subscribed before me on this 4 day of November 2016, at 10:20 a.m. p.m. in Fort Worth, Texas.

JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A

Items Seized by Texas State Comptroller-CID

1. Ten (10) boxes of paper business records containing: sales reports, invoices, receipts, employee work schedules, Federal and State tax documents, bank and credit card statements, etc.

2. One (1) Dell Optiplex 3020 desktop computer with service tag 2HC5H02, containing a Samsung SSD 840 EVO 250GB Model MZ-7TE250 serial number S1DBNSBF894472J and a Seagate Barracuda 500GB serial number Z3TXXK3Z.

3. One (1) Intel D945GCCR desktop computer serial number BTCR7090DAE8 containing a Seagate Barracuda 1OOOGB hard drive Model ST 1000DM003 with serial number Z1DBN10N.

4. One (1) Hewlett-Packard Compaq DC500 SFF desktop computer containing a Hitachi Deskstar model HDS721680PLA380 80GB hard drive with serial number PVFB04ZEU862KE.

5. One (1) Dell Vostro desktop computer service tag F2MR8V1 containing a Seagate Barracuda 160GB hard drive model ST3160815AS with serial number 5RXOPNRD.

6. One (1) WD 1 TB My Passport Ultra USB hard drive with serial number WXE1 E14CPSK3.

7. Two (2) unlabeled compact disks

8. One (1) Emprex 2.0 GB Flash drive

9. One (1) compact disk labeled BTP-2002NP Installation CD

10. One (1) Scandisk Cruzer 8GB USB drive SDCZ36-008G/BI1111WZON

11. One (1) compact disk labeled Samsung Solid State Drive Manual & Software

12. One (1) Sony CD-R compact disks labeled 1-15-13; 1-1-2013;

13. Six (6) Maxell CD-R compact disks labeled: 11-29-10; 1-20-2012; 8-17-10; 2-18-10; 1-30-09 Ug; 9-16-08 Ug

14. One (1) unlabeled Maxell CD-R compact disk

ATTACHMENT B

Information to be Seized by Law Enforcement Personnel

Property which constitutes evidence of the commission of a criminal offense or which is contraband, fruits of the crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of committing an offense: all in violation of 26 U.S.C. §§ 7201 (tax evasion) and 7206(1) (subscribing to a false return), and 18 U.S.C. § Section 371 (conspiracy to impair, obstruct, and defraud the lawful function of the Internal Revenue Service to ascertain, compute, assess, and collect income taxes and distribute tax refunds) occurring during the period 2010 to January 27, 2015, as follows:

1. Employment records containing copies of employees' identifying information, work schedules, and employment application documents;

2. Items relating to income and expenses of KYL International, LLC and Kevin Chau including Federal and state income and employment tax records;

3. Computers and printers;

4. Point of sale system equipment consisting of computers, software, terminals, display monitors, back up hard drives, POS terminal access cards, credit card readers, identification card software, and accounting software;

5. Point of sale networking equipment consisting of modems, routers, cables, servers;

6. Point of sale data files, all past and present versions of POS software, all supported and unsupported versions of the POS software, any and all encryption keys, license keys, product keys, activation keys, hardware keys, passwords, account login information and manuals. POS data including archive and backup copies including client passwords and account login information, encryption keys and other solutions to security measures;

7. Video surveillance DVRs;

8. Current and prior versions of menu and/or records of meal prices;

9. Financial documents of income and expense items;

10. Items relating to manipulation of sales data;

11. Items relating to communications regarding the reporting of information to: (a) an accountant; or (b) directly to the Internal Revenue Service;

12. Records or documents showing individuals', co-conspirators', and/or victims' identifying information, names, Social Security numbers, dates of birth, telephone numbers, and/or addresses;

13. Telephone records, phone and/or address books, names, addresses, and phone numbers, either written or electronic;

14. Financial institution records of account applications, signature cards, statements, deposit items, cancelled checks, withdrawal items, cash withdrawals, checks to cash, wire transfers, cashier's checks, money orders, traveler's checks, bank checks, official checks, cash advance checks, passbooks, records of safety deposit boxes and keys, investment accounts, foreign bank accounts, credit card accounts, store-value card accounts, prepaid card accounts, investment accounts, and the transfer, expenditure, and obtaining of money;

15. Any decryption key or password that could be used to conceal evidence relevant to the above criminal violations;

16. The software, decryption keys or passwords necessary to view and examine the data obtained through computer files;

17. All of the foregoing items of evidence described in the paragraphs above, whatever form and by whatever means such items may have been created or stored, including any hand-made form, any photographic form or any electrical, electronic, digital or magnetic form, such as any information on an electronic, digital or magnetic storage device like a floppy diskette, hard disk, backup media, CD-ROM, thumb-drive, optical disc, electronic dialer, electronic notebook, as well as printouts or readouts from any digital or magnetic storage device;

18. Computer hardware, including data-processing devices (such as central processing units, desktop computers, self-contained "laptop" or "notebook" computers, and Personal Digital Assistants-- PDAs); internal and peripheral storage devices (such as fixed disks, floppy disks, external hard disks, floppy disk drives and diskettes, tape drives and optical storage devices, thumb-drives, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts, that can be used to restrict access to computer hardware (such as physical lock and keys);

19. Computer software, including programs to run operating systems, applications, utilities, compilers, interpreters, video, web browsers, and communications programs;

20. All computer-related documentation including written, recorded, printed, or electronically-stored material which explains or illustrates how to configure or use computer hardware, software, or other related items;

21. All computer passwords and data security devices, including encryption devices, chips and circuit boards.